Tina Wolfson (SBN 174806)
twolfson@ahdootwolfson.com
Theodore W. Maya (SBN 223242)
tmaya@ahdootwolfson.com
Alyssa D. Brown (SBN 301313)
abrown@ahdootwolfson.com
Sarper Unal (SBN 341739)
sunal@ahdootwolfson.com
AHDOOT & WOLFSON, PC
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505
Telephone: (310) 474-9111
Facsimile: (310) 474-8585

Counsel for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

HAYDEN LEE, individually and on behalf of all others similarly situated,

Plaintiff,

v.

META PLATFORMS, INC.; ALPHABET INC.; and GOOGLE LLC,

Defendants.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Hayden Lee ("Plaintiff"), individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to himself and on information and belief as to all other matters, by and through undersigned counsel, brings this Class Action Complaint against Defendants Meta Platforms, Inc. ("Meta"), Alphabet Inc. ("Alphabet"), and Google LLC ("Google") (collectively "Defendants").

NATURE OF THE ACTION

1. This is not the first time consumers are seeking to hold Meta accountable for its collection and tracking of browser activity data without consent through Meta's Pixel Tracking tool. However, this case concerns particularly egregious conduct wherein Meta willfully circumvented protections and security protocols designed to maintain user anonymity and prevent the unauthorized collection and transfer of consumer data across different apps thereby violating numerous consumer protection laws.

2. Under this new scheme, when a consumer visits any of the 5.8 million websites hosting Meta's Pixel Tracking tool,[1] on their Android device it "pass[es] cookies or other identifiers from Firefox and Chromium-based browsers" to the Facebook or Instagram app installed on the consumer's device, which is then matched to user data collected by Facebook or Instagram and forwarded to Meta's servers in order to expand the effectiveness of its targeted advertising business.[2] In other words, Meta created a system, utilizing local ports on Android devices, to collect consumer browsing activity using Meta Pixel and associate that data with data sourced from the logged-in accounts on the installed Facebook and Instagram apps on the Android device. This tracking system affectively de-anonymizes user information and browsing habits, and can do so, even when private browsing modes are enabled on users' devices without their consent.

/ / /

/ / /

/ / /

[1] Dan Goodin, *Meta and Yandex Are De-Anonymizing Android Users' Web Browsing Identifiers*, ARSTECHNICA (June 3, 2025), https://arstechnica.com/security/2025/06/meta-and-yandex-are-deanonymizing-android-users-web-browsing-identifiers/.

[2] *Id*.

3. This tracking mechanism bypasses the Android operating system's "sandbox" feature, which is intended to limit and isolate activity between installed apps, and abuses an Android function that allows local host communication between an app browser and the device's installed apps.[3]

4. Meta specifically targeted Android systems due to Google's imposition of "fewer controls on local host communications and background executions of mobile apps."[4]

5. Meta's main source of income is derived from social media advertisements. Meta's model depends on collecting detailed user data to build behavioral profiles that allow advertisers to reach specific audiences. Ostensibly, the more detailed the user profile, the more valuable the data becomes. By embedding Meta Pixel into 5.8 million websites and bypassing privacy norms and anonymity policies, Meta is able to collect browsing data and associate it with the user's identity thereby increasing the value of its advertising services exponentially.

6. Plaintiff seeks to remedy these harms individually and on behalf of all those similarly situated, whose data privacy was violated as a result of Meta's unlawful conduct.

7. Accordingly, Plaintiff, individually and on behalf of the Class, asserts claims for (1) invasion of privacy, (2) violation of the California Unfair Competition Law Cal. Bus. & Prof. Code §§ 17200, et seq., (4) violation of the Electronic Communications Privacy Act, 18 U.S.C. §§ 2511(1), et seq, and (4) unjust enrichment.

PARTIES

8. Plaintiff Hayden Lee is an adult citizen of the state of Illinois and resides in Chicago, Illinois. Plaintiff Lee is an Android user with an Instagram account who, like other members of the Class, was affected by Meta's unlawful data collection practices.

9. Defendant Meta Platforms, Inc. is a Delaware corporation with its principal place of business located at 1 Meta Way, Menlo Park, California 94025.

10. Defendant Alphabet Inc. is a Delaware limited liability company with its principal place of business at 1600 Amphitheatre Parkway, Mountain View, California 94043.

[3] *Id.*
[4] *Id.*

11. Defendant Google LLC is a Delaware limited liability company with its principal place of business at 1600 Amphitheatre Parkway, Mountain View, California 94043. Google LLC is a wholly owned subsidiary of Alphabet Inc.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(a) and (d), because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of five million dollars ($5,000,000.00) and is a class action in which one or more Class members are citizens of states different from Defendants.

13. The Court has personal jurisdiction over Defendants because Defendants have their principal place of business in California.

14. Venue properly lies in this judicial district because all Defendants reside in this judicial district.

FACTUAL ALLEGATIONS

A. How the Meta Pixel Works

15. In 2015, the Meta Pixel was announced as a tool to refine Meta's targeted advertising.

16. The Meta Pixel is a piece of JavaScript code offered to advertisers (e.g. website operators) to integrate into their websites to collect detailed and granular data for every interaction on a webpage to track visitor activity.[5]

17. The JavaScript code itself is a pixel sized dot, (with a 1 x 1 pixel dimension) nearly invisible to the website visitor. Once a third-party company, advertiser, or other entity installs the Meta Pixel on its website, the information collecting and sharing begins once a visitor clicks a link on the website. Each action taken by the visitor triggers an event that is communicated to a Meta server through a "GET request" performed by the Metal Pixel enabling Meta to build a detailed history of activity per visitor that it can use for more effective ad-targeting. Every action creates a library which

[5] Surya Mattu, Angie Waller, Simon Fondrie-Teitler, & Micha Gorelick, *How We Built a Meta Pixel Inspector*, The Markup (Apr. 28, 2022), https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector.

logs an activity that the third party wants to track. All of these tracked actions are then stored so that the third party can analyze the data collected.[6]

18. On each of the websites embedded with its technology, the Meta Pixel collects and sends information to Meta via scripts running in the background of a person's internet browser. That data is then delivered to Meta in "data packets" labeled with personally identifiable information, including the user's IP address.

19. Importantly, Meta designed the Meta Pixel to receive information about a website user's actions contemporaneously with those actions. This means that as soon as a website user takes any action on a webpage that includes the Meta Pixel, it redirects the user's communications to Meta while communication between the website user and the website is still occurring.

20. According to Meta, the Meta Pixel can collect anything present in http headers, which include "IP addresses, information about the web browser, page location, document, referrer and person using the website"; button click data including "any buttons clicked by site visitors, the labels of those buttons and any pages visited as a result of the button clicks,"; form field names and values if selected by the website owner; and other optional values.[7] The Meta Pixel captures at least seventeen standard events including payment information, registration for events, location search information, purchases, scheduling information such as appointments, what information was searched for, applications, and what content was viewed.[8]

21. Meta touts the "retargeting ability of the Meta Pixel," describing how it can help advertisers create "Custom Audiences," tailoring advertisements to "people who have engaged with the page your pixel is on."[9] Meta also describes how the information harvested by the Meta Pixel can build "Lookalike Audiences," which analyze the information and generate a similar group for targeting. [10] Lookalike Audiences are intended to "have interests, likes, and demographic stats similar

---

[6] *See* Ted Vrountas, *What is the Meta Pixel & What Does it Do?*, Facebook Advertising - Instapage, https://instapage.com/blog/meta-pixel (last visited June 10, 2025).
[7] *Meta Pixel*, Meta, https://developers.facebook.com/docs/meta-pixel/ (last visited June 10, 2025).
[8] Casandra Campbell, *How To Set Up and Use Meta Pixel (Formerly Facebook Pixel)*, Shopify (Jun. 6 2024), https://www.shopify.com/blog/72787269-relax-advertising-on-facebook-just-got-a-lot-easier.
[9] Vrountas, *supra*.
[10] *Id*.

to the people who are already engaging with your website and ads."[11] To do this, Meta naturally needs to receive and analyze these types of information after they are gathered by the Meta Pixel. Meta states that "[t]o create a lookalike audience, our system leverages information such as demographics, interests and behaviors from your source audience to find new people who share similar qualities."[12]

22. Using the data collected through the Meta Pixel process, Meta is able to separate data sets into Custom Audiences, Lookalike Audiences and Core Audiences to increase to effectiveness of Meta's advertising campaigns.

B. The Collection and Use of Data Collected Through Facebook and Instagram

23. Advertising is a significant source of Meta's business revenue. "Substantially all of [Meta's] revenue is currently generated from marketers advertising on Facebook and Instagram."[13] In 2024 alone, Meta reported over $160 billion in annual revenue.[14]

24. Given that its advertising business relies on the effectiveness of its marketing campaigns through the collection and storage of user data, information is ostensibly Meta's biggest and most valuable commodity.

25. However, the data is significantly more robust, and more valuable as a result, when paired with a Facebook or Instagram account.

26. The Meta Pixel system relies heavily on the use of cookies, particularly the third-party cookies to track a visitor's activity which also "enable[s] [Meta] to match [] website visitors to their respective Facebook User accounts."[15] Through this data collection process, Meta is able to provide its marketing partners with direct and detailed insight into individuals' activities, allowing them to track website visitor actions, define custom audiences to better target ads to potential customers,[16] and

---

[11] Vrountas, *supra*, at note 11.

[12] *Facebook Pixel Events*, Meta, https://www.facebook.com/business/m/one-sheeters/facebook-pixel-events (last visited June 9, 2025).

[13] *Meta Platforms Inc. Form 10-K*, U.S. Securities and Exchange Comm'n (Jan. 29, 2025) https://www.sec.gov/Archives/edgar/data/1326801/000132680125000017/meta-20241231.htm#i20db9d0a42f0408c9f8cc4709c09099f_79

[14] *Id*.

[15] *Get Started*, Meta for Developers, https://developers.facebook.com/docs/graph-api/get-started/ (last visited June 10, 2025).

[16] *Id*.

create lookalike audiences to "reach new people who are likely to be interested in [their] business because they share similar characteristics to [the business's] existing customers."[17]

27. Even if a person is not logged in to Facebook at the time, Meta uses personal information a user enters in form fields to match them to their Facebook and/or Instagram profile through a process called Advanced Matching. With this process, Meta collects emails, first and last names, phone numbers, birthdates, and addresses, and then uses that information to connect event tracking data to a specific Facebook profile.

28. In response to congressional questioning in 2018, Meta stated that the Meta Pixel "provide[s] information about users' activities off Facebook—including information about their device, websites they visit, purchases they make, the ads they see, and how they use their services—whether or not they have a Facebook account or are logged into Facebook."[18]

29. Even if a person does not have a Facebook account, has never registered for an account, has never so much as looked at a Facebook or Meta privacy policy, and has no intention to ever join any social media at all, Meta still collects data on that person.

30. When asked by Congress about this maintenance of "shadow profiles" with data of nonusers of Facebook, Mark Zuckerberg responded, "[W]e collect data on people who have not signed up for Facebook for security purposes."[19]

31. Whether the website visitor's information is collected through the Meta Pixel using first- or third-party cookies or compounded with the habits, interests and history gathered from the user's Facebook or Instagram account, the JavaScript code embedded on a website allows only the "tracking of a user under a pseudonym but not their real identity. This is a major drawback on tracking

[17] *About lookalike audiences*, Meta Business Help Center, https://www.facebook.com/business/help/164749007013531?id=401668390442328 (last visited June 10, 2025).

[18] *Social Media Privacy, and the Use and Abuse of Data: Hearing Before the Comm. on Com., Sci., and Transp.*, 94 Cong. 115 (2018) (Post-Hearing Questions).

[19] Taylor Hatmaker, *Zuckerberg Denies Knowledge of Facebook Shadow Profiles*, TechCrunch (Apr. 11, 2018), https://techcrunch.com/2018/04/11/facebook-shadow-profiles-hearing-lujan-zuckerberg/.

as it tenders the attribution of history of activities to a real user (not a pseudonym) almost impossible."[20]

C. Meta De-Anonymizes Android Users by Linking Their Web Activity Collected by Meta Pixel to Their Facebook or Instagram Accounts

32. Meta is well aware that consumers do not want to be spied on while using the internet. Meta has been sued repeatedly for using the Meta Pixel to surreptitiously monitor users' internet activity for Meta's own profit.

33. Because of this, many consumer tech companies design their products to allow users the ability to control the extent to which they are tracked. Privacy norms have arisen in the tech space that facilitate consumer control over information and privacy.

34. For example, as one researcher explained, "[o]ne of the fundamental security principles that exists in the web, as well as the mobile system, is called sandboxing."[21] "Sandboxing" is a technique that isolates mobile apps from one another, including from web browsers, to protect each app and the system as a whole from malicious applications.[22] By default, apps can't interact with each other and have limited access to the operating system. As Google explains to its users on its Android development site, "[i]f app A tries to do something malicious, such as read app B's data or dial the phone without permission, it's prevented from doing so because it doesn't have the appropriate default user privileges . . . . The sandbox is simple, auditable, and based on decades old . . . separation of processes and file permissions."[23]

35. To put this more simply, an app installed on an Android phone is not supposed to be able to access data collected from or on websites, and vice versa. "You run everything in a sandbox,

[20] Paschalis Bekos et al., *The Hitchhiker's Guide to Facebook Web Tracking with Invisible Pixels and Click IDs* (Apr. 2023), https://dl.acm.org/doi/pdf/10.1145/3543507.3583311

[21] Goodin, *supra.*

[22] *See Application Sandbox*, Android, https://source.android.com/docs/security/app-sandbox (last visited June 10, 2025).

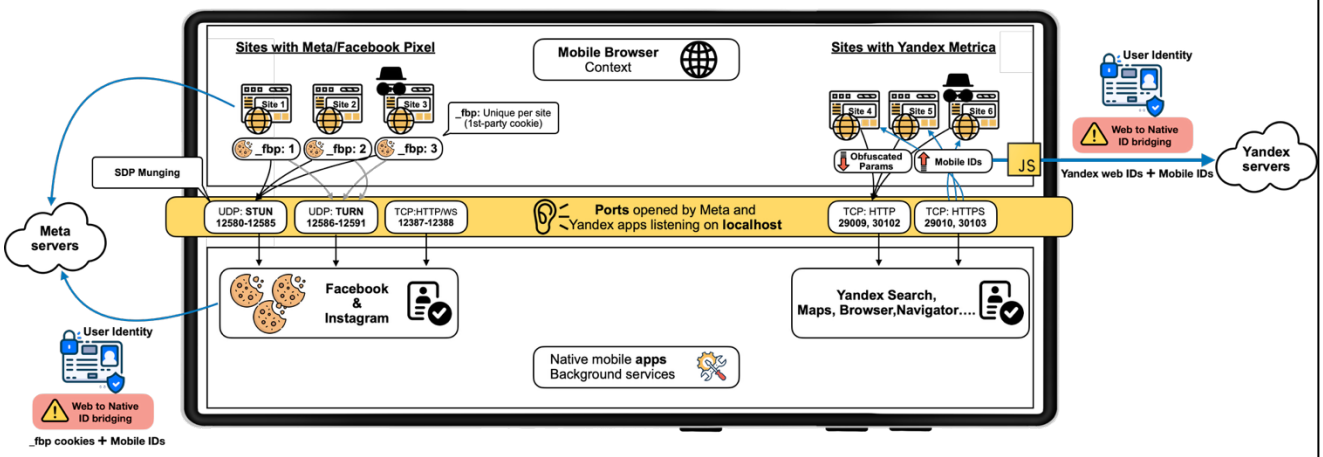
[23] *Id*.

and there is no interaction within different elements running on it."[24] This "cut[s] off access to sensitive data or privileged system resources."[25]

36. For Android users, however, Meta has circumvented the inherent privacy and security protections put in place by Google through Chrome and Android and found ways to collect data that is anything but anonymous.

37. Beginning in September 2024 and continuing through at least June 2, 2025, Meta "abus[ed] legitimate Internet protocols [and platform capabilities], causing Chrome and other browsers [on Android mobile phones] to surreptitiously send unique identifiers to native apps installed on a device."[26]

38. This abuse allowed Meta to "bypass core security and privacy protections provided by both the Android operating system and browsers that run on it," enabling Meta to "pass cookies or other identifiers from [websites with the Meta Tracking Pixel loaded on] Firefox and Chromium-based browsers to native Android apps for Facebook [and] Instagram . . . apps, tying "that vast browsing history to the account holder logged into the app."[27]



[24] Goodin, *supra*.
[25] *Id*.
[26] *Id*.
[27] *Id*.

39. In other words, when an Android user accesses a website on their mobile device where the Meta Tracking Pixel is installed—and if the Android user has the Facebook or Instagram app installed on their device—Meta abuses localhost communication sockets typically "used for legitimate purposes such as web development"[28] to share the fbp values generated on the web browser that Meta uses to tie browsing information with the native apps where users are logged in, hence persistently and "effectively de-anonymizing users' browsing habits on sites containing these trackers."[29]

40. This process renders the browsing history of Android users completely identifiable and more comprehensive than intended, as Meta collects a user's browsing information and links the browsing information to personally identifiable information like full name, e-mail address, and other contact information provided on Facebook and Instagram profiles that is not anonymous. And, of course, Meta profits considerably from this data collection, as Meta's advertising business depends on compiling as much data about users as possible to enable the greatest precision for ad targeting.

41. Incredibly enough, this process enables Meta to "link pseudonymous web identities with actual user identities, even in private browsing modes."[30]

42. Meta specifically targets "only Android users" through this process.[31] However, "similar data sharing between iOS browsers and native apps is technically possible. iOS browsers, which are all based on WebKit, allow developers to programmatically establish localhost connections and apps can listen on local ports. It is possible that technical and policy restrictions for running native apps in the background may explain why iOS users were not targeted by these trackers."[32]

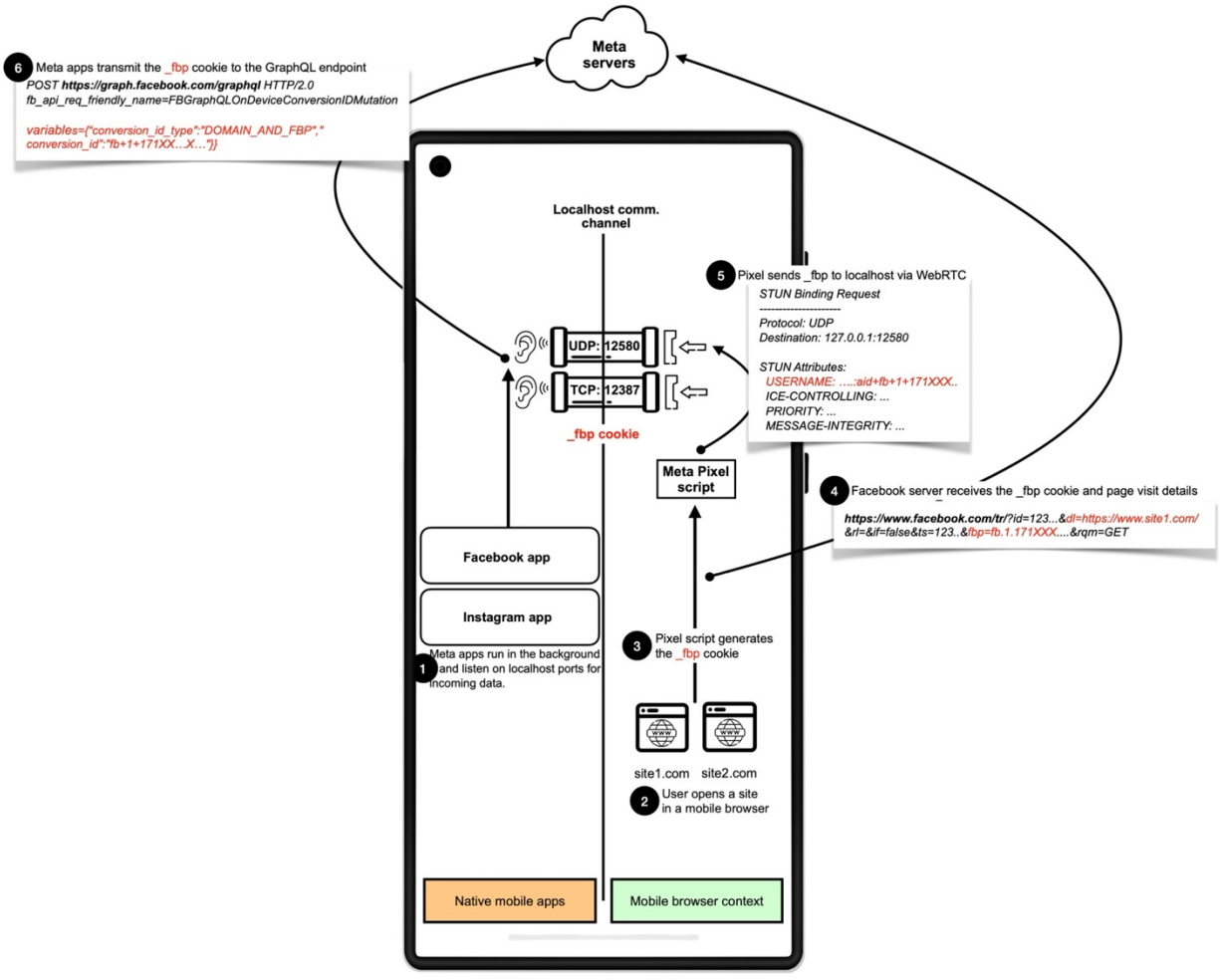
43. The technical flow of Meta's process is as follows[33]:

- The user opens the native Facebook or Instagram app, which eventually is sent to the background and creates a background service to listen for incoming traffic on a TCP port and a UDP port. Users need to be logged in with their credentials on the apps but they remain perpetually logged in whilst the apps are running in the background.

---

[28] Aniketh Girish et al., *Disclosure: Covert Web-to-App Tracking via Localhost on Android* (last updated June 3, 2025), https://localmess.github.io/#faq (last visited June 10, 2025).
[29] Goodin, *supra*.
[30] *Id*.
[31] *Id*.
[32] Girish et al., *supra*.
[33] Goodin, *supra*.

- The user opens their browser and visits a website that hosts the Meta Pixel.
- At this stage, some websites wait for users' consent before embedding Meta Pixel. However, research indicates that a majority of websites do not ask for users' consent.
- The Meta Pixel script is loaded and the _fbp cookie is sent to the native Instagram or Facebook app. The Meta Pixel script also sends the _fbp value in a request to https://www.facebook.com/tr along with other parameters such as page URL (dl), website and browser metadata, and the event type (ev) (e.g., PageView, AddToCart, Donate, Purchase).
- In the final step, the Facebook or Instagram apps receive the _fbp cookie from the Meta JavaScripts running on the browser and transmits it to the GraphQL endpoint along with other persistent user identifiers, linking users' fbp ID (web visit) with their Facebook or Instagram account.



44. To again distill this flow, Meta "insert[ed] key_fbp cookie content into" "a real-time peer-to-peer communication protocol commonly used for making audio or video calls in the browser," "caus[ing] the browser to send that data … to the Android local host, where the Facebook or Instagram app can read it and link it to the user."[34] This means Meta is de-anonymizing and linking Android users' browsing information to their Facebook and Instagram accounts in real time.

45. This means that Meta was able to correlate the _fbp cookie—which is an ostensibly anonymous browser identifier—with the account of a logged in Instagram or Facebook user.

46. This communication was not visible to users, did not seek user consent, and was able to bypass Incognito Mode, cookie clearing, and Android permission mechanisms.

47. Meta's tracking technology transmitted intercepted data instantaneously along with persistent user identifiers stored within those applications—effectively de-anonymizing users and linking their browsing activity to their Meta profiles.

48. When an Android user navigated to a website with the Meta Pixel embedded in it, the Meta Pixel instructed the user's browser to send a separate message to Meta's external servers simultaneously. This separate message included data collected by the Pixel as well as cookie data. At the same time, cookie data was passed through the Android device's local capabilities and paired with the identity of the logged-in user of the Facebook or Instagram applications.

49. Meta accomplished this by abusing access to "local host sockets" which allow applications, such as Facebook and Instagram, to "listen" and read data transmitted by the browsers.[35]

50. Due to this breach, when Android users with a Meta application installed on their device visited websites the Meta Pixel sent "the _fbp value in a request to https://www.facebook.com/tr along with other parameters such as page URL (dl), website and browser metadata, and the event type (ev) (e.g., PageView, AddToCart, Donate, Purchase)."[36] Depending on the users' activity, this means that sensitive information such as healthcare searches, financial data inputted in form fields, and any other private activities users conducted online on their devices would be transmitted to Meta and linked with

[34] *Id*.
[35] Girish et al., *supra*.
[36] *Id*.

their identities stored on their Meta applications. This invasion is especially harmful as Meta operates a "real identity" platform where users are required to create "one account using the name they go by in everyday life that represents their authentic identity."[37]

D. Google's Failure to Secure Users' Privacy in Android Systems

51. Android is a mobile operating system developed by Google that powers billions of mobile devices globally, including smartphones, tablets, and wearable devices.[38] As of 2022, approximately 133 million individuals in the United States owned a smartphone powered by the Android operating system in the United States.[39]

52. Google pre-installs a suite of software on Android devices including the Chrome web browser. Consumers are additionally able to download third-party apps from the Google Play store including the Facebook and the Instagram mobile apps.

53. Google ensures that consumer's devices are safe when they download third-party apps on their Android devices from the Google Play store. In its article, "How we keep Google Play safe for users and developers" Google explains how it is "continually working on ways to weed out harmful apps and keep users, and developers, safe."[40]

54. Google knows and appreciates that consumers' phone data is sensitive and understands the importance of keeping consumer data safe and mobile apps downloaded from its own Google Play store free of malicious software and vulnerabilities. Google proclaims: "Your life is on your phone: your financial information, personal data, photos, and more. So Pixel is built with security at its core. Pixel hardware and software work together to help keep your phone and data private, safe, and secure."[41]

---

[37] *Authentic Identity Representation*, META, https://transparency.meta.com/policies/community-standards/authentic-identity-representation (last visited June 10, 2025).
[38] *See* Android, https://www.android.com/ (last visited June 10, 2025).
[39] iPhone vs Android Statistics, BACKLINKO.COM (last updated Mar. 31, 2025), https://backlinko.com/iphone-vs-android-statistics (last visited June 10, 2025).
[40] *How we help keep Google Play safe for users and developers*, Google, https://safety.google/intl/en_us/stories/google-play-safety/ (last visited June 10, 2025).
[41] *Id.*

55. However, Google failed to keep its promise to its users and to install measures to maintain their privacy.

56. Google's failure to secure its Android software to prevent unauthorized access to consumers' devices by Meta is unacceptable and has led to a violation of its users' privacy and subjected them to actual harm and put them at a future risk of harm.

57. Google has implemented an "overly permissive" Android design that "allows Meta Pixel and Yandex Metrica to send web requests with web tracking identifiers to specific local ports that are continuously monitored by the Facebook, Instagram, and Yandex apps."[42]

58. Specifically, Google's decision to allow third-party developers to access specific local ports should have been, and upon information and belief was not, supplemented with a security protocol to ensure such access was not misused. Due to this failure, Meta was able to exploit Android's software and de-anonymize users and their browsing activity with no sufficient oversight from Google.

59. Google knew, or should have known, that by failing to monitor this access it had allowed a core vulnerability in the Android software that would allow developers such as Meta to identify users and track their online activity without consent.

60. Google has falsely claimed that Android allows users to "choose when to share certain sensitive data with apps you download."[43] It is now clear that users had no control over their privacy while Google negligently and/or recklessly allowed developers to manipulate fundamental aspects of Android's software without corresponding safeguards. Google's additional claims that "Android minimizes and de-identifies your data from intelligent features. And restricts access to technically ensure your privacy and safety," was also false.

61. Indeed, Google sold its Pixel phones with the false promise that "[a]ll Pixel devices are designed to respect your privacy . . . we ensure the privacy and safety of your data by minimizing the

[42] Goodin, *supra*.

[43] *Android Privacy Settings and Permissions*, Android, https://www.android.com/safety/privacy/#safety-privacy-dashboard (last visited June 10, 2025).

amount of data stored, **de-identifying it so that the data is not linked to you**, and restricting its access altogether."[44]

62. Google can and should have done more to protect Android users from Meta's malicious attack and unauthorized tracking by securing its Android software. Google failed Android users and violated the privacy promises it had made to them in exchange for their business.

63. Google's failures are especially egregious when considering that Yandex has been exploiting these vulnerabilities since at least 2017.

PLAINTIFF'S EXPERIENCE

64. Between September 2024 and the present, Plaintiff visited several websites on his Android mobile phone where the Meta Tracking Pixel was installed.

65. When Plaintiff visited these websites on his Android phone, Plaintiff had the Instagram app installed on his phone.

66. Unbeknownst to Plaintiff, when Plaintiff visited these websites, everything Plaintiff did on these websites—e.g., what articles Plaintiff viewed, what things Plaintiff searched for and the specific search terms—and Facebook ID were collected by Meta in real time using the Meta Tracking Pixel. This was so regardless of what the websites may or may not have configured Meta to collect.

67. Further, when Plaintiff visited these websites, and unbeknownst to Plaintiff, Meta sent a separate signal to itself that allowed Meta to tie Plaintiff's browsing information to the information he submitted on his Facebook and Instagram profiles (his name, address, e-mail address, etc.) in real time, thus de-anonymizing and identifying Plaintiff and his browsing information in real-time.

CLASS ALLEGATIONS

68. Plaintiff brings this action on behalf of himself and the following Class pursuant to Federal Rule of Civil Procedure 23(a) and (b):

> All Android mobile device users in the United States with a Facebook or Instagram account who (i) have the Facebook or Instagram app installed on their Android phone, (ii) visited on their Android mobile phones a website between September 2024 and June 2, 2025 where the Meta

[44] *Google Pixel Privacy and Security Features*, GOOGLE, https://safety.google/pixel/ (last visited June 10, 2025) (emphasis added).

Tracking Pixel was installed, and (iii) whose browsing information was collected by Meta.

69. Excluded from the Class are Defendants and their affiliates, officers, directors, assigns, successors, and the Judge(s) assigned to this case.

70. **Numerosity:** While the precise number of Class members has not yet been determined, members of the Class are so numerous that their individual joinder is impracticable, as the proposed Class appears to potentially include millions of members who are geographically dispersed.

71. **Typicality:** Plaintiff's claims are typical of Class members' claims. Plaintiff and all Class members were injured through Defendants' uniform misconduct, and Plaintiff's claims are identical to the claims of the Class members they seek to represent. Accordingly, Plaintiff's claims are typical of Class members' claims.

72. **Adequacy:** Plaintiff's interests are aligned with the Class they seek to represent, and Plaintiff has retained counsel with significant experience prosecuting complex class action cases, including cases involving alleged data privacy violations. Plaintiff and undersigned counsel intend to prosecute this action vigorously. The Class's interests are well-represented by Plaintiff and undersigned counsel.

73. **Superiority:** A class action is the superior—and only realistic—mechanism to fairly and efficiently adjudicate Plaintiff's and other Class members' claims. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for Class members individually to effectively redress Defendants' wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

74. **Commonality and Predominance:** The following questions common to all Class members predominate over any potential questions affecting individual Class members:

- whether Defendants engaged in the wrongful conduct alleged herein;
- whether Defendants acted intentionally in violating Plaintiffs' and Class members' rights under the ECPA and the UCL;
- whether Defendants' conduct alleged herein violated privacy rights and invaded Plaintiff's and Class members' privacy;
- whether Defendants' conduct alleged herein constitute egregious breaches of social norms; and
- whether Plaintiff and Class members are entitled to damages, equitable relief, or other relief and, if so, in what amount.

75. Given that Defendants engaged in a common course of conduct as to Plaintiff and the Class, similar or identical injuries and common law and statutory violations are involved, and common questions outweigh any potential individual questions.

CAUSES OF ACTION

COUNT I

Invasion of Privacy
(On Behalf of Plaintiff and the Class)

76. Plaintiff realleges and incorporates all previous allegations herein.

77. Plaintiff brings this claim individually and on behalf of the Class against Defendants.

78. Plaintiff and Class members had a reasonable expectation of privacy in their browsing activity on their Android devices. Plaintiff and Class members communicated information that they intended for only the websites they visited to receive and that they understood Defendants would not track and that their browsing activity would be kept private.

79. Defendants' tracking and disclosure of that information without the knowledge and consent of Plaintiff and Class members is an intrusion on Plaintiff's and Class members' solitude and seclusion.

80. Meta violated Plaintiff's and Class members' privacy through intentional and malicious exploitation of software on their Android devices.

81. The level of invasion and systemic surveillance of Plaintiff and Class members is highly offensive to a reasonable person. Meta designed a malicious code to exploit vulnerabilities in Android software that allowed Meta to collect Plaintiff's and Class members' online activity over time and connect

it with their identities. Meta then sold Plaintiff's private information and identities for the purpose of profiting from targeted advertising.

82. Defendants profited from this invasive surveillance of Android users through sales of targeted advertising.

83. Defendants obtained Plaintiff's and Class members' information under false pretenses and/or exceeded its authority to obtain such information.

84. As a result of Defendants' actions, Plaintiff and Class members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

85. Plaintiff and Class members have been damaged as a direct and proximate result of Defendants' invasion of their privacy and are entitled to just compensation, including monetary damages.

86. Plaintiff and Class members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiff and Class members for the harm to their privacy interests because of Defendants' intrusions upon Plaintiff's and Class members' privacy.

87. Plaintiff and Class members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendants' actions, directed at injuring Plaintiff and Class members in conscious disregard of their rights. Such damages are needed to deter Defendants from engaging in such conduct in the future.

88. Plaintiff also seeks such other relief as the Court may deem just and proper.

COUNT II
Violations of the California Unfair Competition Law
Cal. Bus. & Prof. Code §§ 17200, et seq. ("UCL")
(On Behalf of Plaintiff and the Class)

89. Plaintiff realleges and incorporates all previous allegations herein.

90. Plaintiff brings this claim individually and on behalf of the Class against Defendants.

91. California's Unfair Competition Law ("UCL") prohibits any "unlawful, unfair, or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200.

92. Meta engaged in unlawful business practices in connection with its collection and dissemination of users' de-anonymized data as alleged in detail herein.

93. Google engaged in unlawful business practices in connection with its misleading advertising regarding the safety and privacy protections available on Android devices, including Android users' ability to stay anonymous online.

94. The acts, omissions, and conduct of Defendants as alleged herein constitute "business practices" within the meaning of the UCL.

95. Defendants violated the "unlawful" prong of the UCL by violating, inter alia, Plaintiff's and Class members' rights to privacy and the ECPA.

96. Defendants' acts, omissions, and conduct also violate the unfair prong of the UCL because those acts, omissions, and conduct, as alleged therein, offended public policy and constitute immoral, unethical, oppressive, and unscrupulous activities that caused substantial injury, including to Plaintiff and Class members.

97. The harm caused by Defendants' conduct outweighs any potential benefits attributable to such conduct and there were reasonably available alternatives to further Defendants' legitimate business interests other than Defendants' conduct described therein.

98. As a result of Defendants' violations of the UCL, Plaintiff and Class members are entitled to injunctive relief. This is particularly true since Meta has shown the ability and willingness to engage in the alleged conduct and Google has failed to properly secure Android at least since 2017.

99. As a direct and proximate result of Defendants' violations, Plaintiff and Class members have suffered injury in fact and lost money by having their browsing activity collected and sold to third parties without their consent.

COUNT III
Violations of the Electronic Communications Privacy Act
18 U.S.C. § 2511(1), *et seq*
(On Behalf of Plaintiff and the Class)

100. Plaintiff realleges and incorporates all previous allegations herein.

101. Plaintiff brings this claim individually and on behalf of the Class against Defendants.

102. The Electronic Communications Privacy Act ("ECPA") prohibits the intentional interception of the content of any electronic communication. 18 U.S.C. § 2511.

103. The ECPA protects both the sending and the receipt of communications.

104. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

105. The transmission of Plaintiff's and Class members' website page visits, browsing and search information, and persistent identifiers each qualify as a "communication" under the ECPA's definition of 18 U.S.C. § 2510(12).

106. The transmission of this information between Plaintiff and Class members, on the one hand, and each website with which they chose to exchange communications, on the other hand, are "transfer[s] of signs, signals, writing, . . . data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

107. The ECPA defines "contents," when used with respect to electronic communications, to "include[] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8).

108. The ECPA defines an interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

109. The ECPA defines "electronic, mechanical, or other device," as "any device . . . which can be used to intercept a[n]…electronic communication." 18 U.S.C. § 2510(5).

110. The following instruments constitute "devices" within the meaning of the ECPA: (i) The Meta Tracking Pixel; (ii) The code that enabled Meta to link browsing information with Facebook and Instagram profiles; and (iii) Any other tracking code or SDK used by Defendants.

111. Plaintiff and Class members' interactions with each website are electronic communications under the ECPA.

112. By utilizing the methods described herein, Defendants intentionally intercepted and/or endeavored to intercept the electronic communications of Plaintiff and Class members in violation of 18 U.S.C. § 2511(1)(a).

113. Defendants then monetized and thus used the intercepted communications for advertising purposes. By intentionally using, or endeavoring to use, the contents of Plaintiff's and Class members' electronic communications, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendants violated 18 U.S.C. § 2511(1)(d).

114. Defendants were not acting under the color of law to intercept Plaintiff's and Class members' electronic communications.

115. Plaintiff and Class members did not authorize Defendants to acquire the content of their communications for purposes of invading Plaintiffs' and Class members' privacy.

116. Plaintiff and Class members had a reasonable expectation that Defendants would not intercept their communications and sell their data for advertising purposes without their knowledge or consent.

117. The websites Plaintiff and Class members visited did not authorize or consent to Defendants' conduct, given Defendants' conduct constituted an abuse of Android security protocols and a violation of Google's terms.

118. The foregoing acts and omissions therefore constitute numerous violations of 18 U.S.C. §§ 2511(1), et seq.

119. As a result of every violation thereof, on behalf of themselves and Class members, Plaintiff seeks statutory damages of $10,000 or $100 per day for each violation of 18 U.S.C. §§ 2510, et seq. under 18 U.S.C. § 2520.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

120. Plaintiff realleges and incorporates all previous allegations herein.

121. Plaintiff brings this claim individually and on behalf of the Class against Defendants.

122. Defendants have wrongfully and unlawfully trafficked in the Plaintiff's and Class members' personal information and other personal data without their consent for substantial profits.

123. Plaintiff's and Class members' personal information and data have conferred an economic benefit on Defendants, in that Defendants used their unauthorized connection with Android

communication channels to link Facebook and Instagram accounts with browsing activity, this rendering the browsing activity de-anonymous and identifiable, and more valuable to advertisers. Defendants also conducted this activity without consent.

124. Defendants have been unjustly enriched at the expense of Plaintiff and Class members and have unjustly retained the benefits of their unlawful and wrongful conduct.

125. It would be inequitable and unjust for Defendants to be permitted to retain any of the unlawful proceeds resulting from its unlawful and wrongful conduct.

126. Plaintiff and Class members accordingly are entitled to equitable relief including restitution and disgorgement of all revenues, earnings, and profits that Defendants obtained as a result of their unlawful and wrongful conduct.

127. When a defendant is unjustly enriched at the expense of a plaintiff, the plaintiff may recover the amount of the defendant's unjust enrichment even if plaintiff suffered no corresponding loss, and plaintiff is entitled to recovery upon a showing of merely a violation of legally protected rights that enriched a defendant.

128. Defendants have been unjustly enriched by virtue of their violations of Plaintiff's and Class members' legally protected rights to privacy as alleged herein.

129. Defendants were aware of the benefit conferred by Plaintiff and Class members. Indeed, Meta deliberately exploited the Android communication channels to link browsing information to Facebook and Instagram profiles. Defendants therefore acted in conscious disregard of the rights of Plaintiff and Class members and should be required to disgorge all profit obtained therefrom to deter Meta and others from committing the same unlawful actions again. Google deceived consumers regarding the security measures of the Android system and failed to protect its users privacy.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of the Class, by and through undersigned counsel, respectfully requests that the Court grant the following relief:

A. Certify this case as a class action pursuant to Fed. R. Civ. P. 23, and appoint Plaintiff as class representative and undersigned counsel as class counsel;

B. Award Plaintiff and Class members actual and statutory damages to the maximum extent allowable;

C. Award Plaintiff and Class members pre-judgment and post-judgment interest to the maximum extent allowable;

D. Award Plaintiff and Class members reasonable attorneys' fees, costs, and expenses, as allowable; and

E. Award Plaintiff and Class members such other favorable relief as allowable under law or at equity.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all issues so triable.

Respectfully submitted,

Dated: June 10, 2025

/s/ Tina Wolfson

Tina Wolfson (SBN 174806)
twolfson@ahdootwolfson.com
Theodore W. Maya (SBN 223242)
tmaya@ahdootwolfson.com
Alyssa D. Brown (SBN 301313)
abrown@ahdootwolfson.com
Sarper Unal (SBN 341739)
sunal@ahdootwolfson.com
AHDOOT & WOLFSON, PC
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505
Telephone: (310) 474-9111
Facsimile: (310) 474-8585

Class Counsel for Plaintiff and the Proposed Class